ABSTRACT

This invention uses probabilistic correlation techniques to increase sensitivity, reduce false alarms, and improve alert report quality in intrusion detection systems. In one preferred embodiment, an intrusion detection system includes at least two sensors to monitor different aspects of a computer network, such as a sensor that monitors network traffic and a sensor that discovers and monitors available network resources. The sensors are correlated in that the belief state of one sensor is used to update or modify the belief state of another sensor. In another embodiment of this invention, probabilistic correlation techniques are used to organize alerts generated by different sensors in an intrusion detection system. By comparing features of each new alert with features of previous alerts, rejecting a match if a feature fails to meet or exceed a minimum similarity value, and adjusting the comparison by an expectation that certain feature values will or will not match, the alerts can be grouped in an intelligent manner.

20302828.doc